AIR WAR COLLEGE

AIR UNIVERSITY

AIR FORCE CYBER MISSION ASSURANCE

SOURCES OF MISSION UNCERTAINTY

by

Ivan Herwick, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lt Col Benjamin Nelson

06 April 2017

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Ivan M. Herwick is currently a student at the Air War College, Air University, Maxwell Air Force Base, Alabama. He entered the Air Force in 1997 as a graduate of the United States Air Force Academy and is currently a cyber operations officer. Lt Col Herwick has served at squadron, group, wing, major command, Headquarters Air Force, and Joint Staff levels. This includes commanding the 386th Expeditionary Communications Squadron at Ali Al Salem AB, Kuwait, and the 375th Communications Squadron at Scott AFB, Illinois. He attended intermediate developmental education at the United States Army's Command and General Staff College at Fort Leavenworth, Kansas. Lt Col Herwick holds a bachelor of science degree in Computer Science from the United States Air Force Academy and a master's degree in Computer Resources and Information Management from Webster University.

Abstract

Much of the cyber capabilities that enable mission owners to function are outside their influence and often outside their visibility. This situation exists because of the confusing nature of "cyber," how the Air Force has evolved cyber capabilities, significant institutional disconnects, what a mission owner wants, and the nature of risk management. The consequences of these issues are more than academic concerns as they have contributed to tangible issues throughout the Air Force. At present, it appears that there is a disconnect between the state of cyber capabilities from the perspective of the user and that of key leaders in positions to exert great influence on the future of cyber in the Air Force. While the Air Force likely cannot afford to meet every organization's desired level of performance, it can ensure that it closes the gap between actual performance and the assessed level of performance—ensuring that programmatic and operational decisions are based on a shared understanding of reality. Such transparency and shared understanding will also provide additional accountability at all levels of cyber operations. This will facilitate informed discussions that can ensure authorities and responsibilities remain aligned with mission requirements, but still balanced with accountability for performance.

> "All [Airmen] performing missions need information to make the right decision – whether it's putting bombs on target, dropping humanitarian aid, uploading a software patch to [a] satellite, designing base-level IT infrastructure, or even prescribing the right medical treatment."
>
> Air Force Information Dominance Flight Plan 2015[1]

Introduction

A portion of the Air Force's cyber capabilities focused on attacking and exploiting adversary networks, but the majority exists to provide support to non-cyber functions. The Air Force uses information technology (IT) to enable efficiency and effectiveness for every mission area, ranging from weapons systems to installation support and business functions. The Air Force tasked 24th Air Force (24 AF) with the operation of Air Force cyber capabilities, but does not have effective visibility into all of the cyber terrain that supports these mission areas. In addition, these mission activities often have little insight into the status of services managed or provided by 24 AF and functional communities. Mission owners must assume that the providers of a capability are going to deliver whenever they need the service.

Organizations and missions are increasingly dependent on cyber resources, but those capabilities are subject to disruption, degradation, and failure.[2] Critical information required to support decisions and mission owners face a range of threats from adversary action to environmental conditions.[3] However, much of the cyber capabilities that enable mission owners to function are outside their influence and often outside their visibility. This situation exists because of the confusing nature of *cyber*, how the Air Force has evolved cyber capabilities, significant institutional disconnects, what a mission owner wants, and the nature of risk management. The consequences of these issues are more than academic concerns as they have generated tangible consequences throughout the Air Force.

Much of the discussion in this paper focuses on the unclassified portion of the Air Force Network (AFNet), otherwise known as the Nonsecure Internet Protocol Router Network (NIPRNET), to improve access to relevant information and facilitate distribution. Focusing on NIPRNET may generate concerns that the discussion focuses excessively on a primarily administrative (and therefore less important) network, where other networks, like the SECRET Internet Protocol Router Network (SIPRNET), are more mission focused. However, classification concerns and the general programmatic state of SIPRNET drove the use of NIPRNET and specifically the AFNet as the primary focus. Regardless, many of the concepts discussed are network-agnostic, since the true mission requirement is access to information and the ability to exchange data as needed.

As cyberspace is not the exclusive domain of the cyber operator, this paper describes issues that are the concern of more than a cyber audience. It is not mere advocacy for additional resources against cyber capabilities, nor is it a suggestion that the capabilities discussed are inherently governmental in nature—those are important issues, but outside the scope of this paper. It should inform leaders, mission owners, and functional communities within the Air Force on issues that exist within the Air Force enterprise and facilitate a discussion on how to manage and invest in cyber and cyber-enabled capabilities. Without common understanding, it is difficult to have consensus on what capabilities are the most important to mission owners, what performance levels they require, and how to resource capabilities appropriately. The disconnects outlined in this paper undercut the effectiveness of that dialogue.

GENESIS OF CYBER CONFUSION

Inconsistent, Misunderstood, and Evolving Terminology

"If you wish to converse with me, define your terms"

Voltaire[4]

Understanding the term *cyber* can be an exercise in confusion. It is a relatively new addition to the military vocabulary and while it is common to use conversationally, that usage is not always based on specific definitions. As a result, it finds common usage in place of legacy terms, while seemingly interchangeable with an array of other words. In fact, the Department of Defense dictionary does not have an entry for *cyber* specifically, but a close look at the definitions surrounding cyber reveals a complex universe of terms and potential confusion.

While cyber may not be a defined word, it should be accepted as a colloquial version of *cyberspace* which the Department of Defense (DoD) defines as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] Based on this definition, cyber is something more than just *information technology*, but less than the *information environment* which is defined as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[6] To expand to how cyberspace is operated and maintained, joint doctrine divides cyberspace operations into offensive, defensive, and DoD Information Network (DODIN) operations.[7] While the first two are self-explanatory, the third consists of "operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information network."[8] This highlighted difference between *networks*

and *information network* is left somewhat unexplained, but DODIN is an inclusive term that expands on technical aspects of *cyberspace* to include the software, services, support personnel, and processes for handling information.[9] From the interrelation of these various terms, *information environment* and *information network* appear very similar, suggesting that networks are closer to the definition of *cyberspace* or even *information technology*. These definitions confusingly make cyber both an inclusive term (e.g., cyberspace operations), but also exclusive of anything non-technical (e.g., cyberspace).

Guidance to the DoD on how to develop capabilities in and for cyberspace add additional insight into how to use these key terms. The DoD developed its Cyber Strategy to "guide the development of DoD's cyber forces and strengthen our cyber defense and cyber deterrence posture."[10] It focuses on "defending DoD networks, systems and information," U.S. national interests, and providing operational capability to warfighters.[11] To relate this to the terms and definitions above, this suggests that the DoD's priorities are on capabilities that support the offensive and defensive elements of cyberspace operations. This stands in contrast with the Air Force's Information Dominance Flight Plan which refers to the "systems and data of cyberspace" and uses a combined "IT/cyberspace" term, while also using the terms IT and cyberspace separately.[12] The document leaves the impression that the terms are potentially interchangeable.

In addition to confusion created by terminology usage in doctrine and guidance, the Air Force has repeatedly changed the terms associated with installation-level functions, which is where a significant portion of Air Force personnel interact with cyberspace. *Client Support Administrator* replaced *Work Group Manager*, before the Air Force moved to the term *Client Support Technician* to reflect the title of the Air Force Specialty Code (AFSC) that provides first-line troubleshooting for users and their systems. To gain efficiencies in supporting calls

from customers, the Air Force established the Enterprise Service Desk which was a consolidated call center that the Air Force later disbanded—referring the user back to their local installation for support. To comply with a DoD-directed name change, the *Cybersecurity Office* and unit *Cybersecurity Liaisons* replaced the *Information Assurance Office* and the unit *Information Assurance Officers*.[13] Within the Air Force, the organizations that conduct most cyber-related functions are *communications*, *network operations*, and *cyber operations* squadrons. The officer career field with predominant responsibility for cyberspace is the 17D (Cyberspace Operations) core AFSC which replaced the *Communications Officer* moniker. A certain portion of these officers are in positions identified for the 17S (Cyber Warfare Operations) AFSC. These officers "[operate] cyberspace weapons systems and [command] crews to accomplish cyberspace, training, and other missions." The remaining officers in positions designated with the 17D (Network Operations) AFSC. These officers also "[operate] cyberspace weapons systems, [employ] cyberspace capabilities, and [command] crews to accomplish cyberspace, training, and other missions."[14] Despite a lack of descriptive difference in the Air Force Officer Classification Directory, as the name implies, the 17S career field addresses the specialized knowledge and skills required to conduct offensive and defensive operations. Adding another term, the enlisted career field responsible for most DODIN operations within the Air Force, the 3D career field, is titled *Cyberspace Support*. The technology of cyberspace evolves quickly, but these terms suggest that policy and organization evolve quickly as well.

It is in this context that audiences consume public statements by leadership throughout the DoD and the Air Force specifically. For example, the DoD Information Technology budget request to Congress for fiscal year 2017 was $38.2 billion, which included $6.8 billion for cyber operations.[15] This is an increase over the previous year's budget request of $36.9 billion, which

included $5.5 billion for "cyberspace operations and activities."[16] While the difference between budget requests and what Congress enacts can vary and it is difficult to compare budget numbers given classified programs that may or may not be included in the numbers, these numbers demonstrate an intent to increase spending on information technology. They also show that the increase is predominantly in cyber operations, which based on the definitions above is mostly offensive and defensive capabilities. The average Airman does not generally see these activities, so they may not see the benefits of increased spending on cyber in their daily tasks.

Cyberspace, as the only domain entirely created by humans, is extraordinarily complex, evolving, and requires a complex language to describe it. Moore's Law is an observation that describes the ever-increasing complexity and capability of computer processors—nearly doubling every two years. However, the term may also loosely apply to the terminology and organization that DoD uses for cyber, which may seem to outpace information technology refresh rates. On the surface, this may seem like a trivial issue; however, the lack of a common terminology contributes to misunderstanding and confusion over what cyber is, what it is not, and what Airmen should expect from a domain that is seeing significant increases in resourcing.

Consolidation and Standardization of Information Technology

To gain efficiencies and improve effectiveness, the DoD and the Air Force continue to consolidate and standardize IT capabilities under initiatives like the Joint Information Environment, the Federal Data Center Consolidation Initiative, and Collaboration Pathfinder. One area where this consolidation is evident is in the restructuring of responsibilities among organizations that have roles in the management and sustainment of information technology. As Figure 1 describes, operation and sustainment of the "Air Force Communications/Cyber

enterprise" requires the efforts of multiple organizations, with the Air Force Installation and Mission Support Center (AFIMSC) being the latest edition.

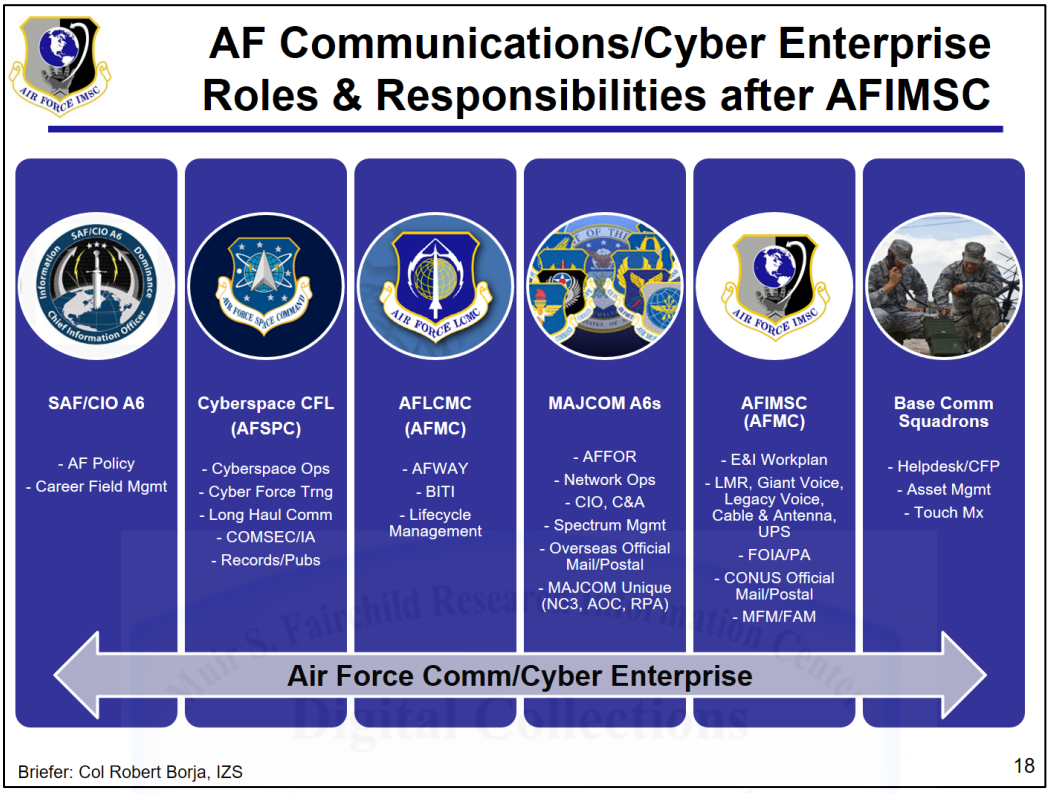

Figure 1. AF Communications/Cyber Enterprise Roles & Responsibilities.[17]

AFIMSC consolidated the major command (MAJCOM) responsibilities for installation and mission support capabilities, which includes base communications.[18] The AFIMSC activated on 6 April 2015 and achieved Full Operating Capability in October 2016, which highlights that this is a recent transition for the communications/cyber enterprise and suggests that processes and relationships among the actors may still be under development.[19] Together these, now six, organizations have primary responsibility for the enterprise, with each having both distinct and overlapping responsibilities. For example, several organizations share responsibility for sustaining and providing the infrastructure that serves as the backbone of the network at each installation. As depicted in Figure 1, the Air Force Life Cycle Management Center (AFLCMC) oversees the Base Information Transport Infrastructure (BITI) program which provides the

"wired cyber network infrastructure at each … base."[20] Additionally, AFIMSC now oversees the Engineering and Installation (E&I) Workplan process, which ensures "the Air Force cyberspace infrastructure is mission ready."[21] These programs traditionally are unable to satisfy every requirement at the base level, so MAJCOMs and base-level organizations often supplement the central programs. Examples exist beyond just infrastructure, but this one example demonstrates the complex relationships among multiple organizations to provide cyber capabilities. While this structure may provide some flexibility, it complicates programmatic trades in the context of the entire enterprise, gives multiple paths for funding capability, and dilutes responsibility for cost and performance.

To provide additional structure to its networks, the Air Force formally designated several weapon systems to provide and secure cyberspace capabilities.[22] Many of the capabilities provided by these weapon systems were already in existence, but transitioning to the weapon system model was done to "help ensure proper management and sustainment of equipment life cycles."[23] Of the six weapon systems designated in 2013, the Air Force Cyber Security and Control System (CSCS) provides much of the network and services that users interact with regularly on the AFNet. CSCS was the next step in a lengthy and complex effort to consolidate the operation of disparate MAJCOM networks.[24] While this may be a better construct than what preceded it, the results demonstrate that the Air Force has not yet realized the expected benefits of weapon system designation. The 561st Network Operations Squadron, one of the primary organizations charged with the operation of the CSCS weapon system, characterized it in late 2016 as having "no baseline," having a sustainment model that "doesn't meet operational need," lacking programmatic processes, and lacking accountability.[25] As the organizational construct for managing the Air Force's networks continues to evolve, the resulting capability must be

monitored to assess the effectiveness of the changes and to ensure the system continues to meet customer needs.

As the above list of organizations involved in the maintenance and operation of the Air Force's cyber capabilities implies, synchronizing authority, accountability, and responsibility is complex. In many cases, the nexus between the organizations listed above and the mission is the installation—the platform from which the Air Force conducts its missions and projects power. In this construct, the communications squadron or the frontline technician is accountable to their local leadership to assure the missions conducted from that installation. As the local cyber operators and maintainers, they represent the primary interface for the entire array of organizations involved in providing cyber-enabled capabilities, regardless if they have the responsibility or authority to address the specific issue. Likewise, where the technician may be responsible for assisting a customer with an issue, the rights delegated to them on the network may limit their ability to be responsive. Taken together, these disconnects provide a source of confusion and perceived distance between mission owners and those that provide and sustain the capabilities that support them.

Institutional Disconnects

To standardize delivery of installation support services, the Air Force developed its Common Output Levels Standards (AF COLS). This program, modeled after the Joint Base COLS program, allows the Air Force to "streamline operations in a fair and consistent manner."[26] In practice, AF COLS is a process that determines desired levels of service and holistically informs planning, programming, budgeting, and execution.[27] AF COLS addresses 43 installation support activities—those functions that are typical to most installations and most of

which are found in the local Mission Support Group.[28] Functions are assigned a number from one to four, with one representing the highest standard. For those functions assigned a four, the Air Force accepts that their performance may be substandard, but still able to meet operational and/or legal requirements.[29] AF COLS allows the Air Force to proactively manage installation support requirements, assess risk at a corporate level, and consistently apply priorities to meet needs and fiscal constraints. For FY17, Cyberspace Operations and Information (CO&I) is a three, the same as its level from FY16 and FY13.[30] For the sake of comparison, Table 1 lists the number of functions by AF COLs level.

Table 1. Count of functions by AF COLS level

AF COLS Level	Description of Standard	Functions at this level
AF COLS 1	"Highest standard"	9 functions
AF COLS 2	"Slightly-reduced standard"	20 functions
AF COLS 3	"Moderately-reduced standard"	10 functions
AF COLS 4	"Greatly-reduced standard"	4 functions

The Air Force must make decisions about how to balance capabilities and budget realities, but an examination of AF COLS gives insight into why the service has cyberspace capabilities that do not meet everyone's expectations: it chose to. As these levels inform the planning and programming process, AF COLS will influence performance levels for several years.

Despite the corporate risk that the Air Force has chosen to accept in this area, 24th Air Force identifies in its mission brief that they achieved 99.999% availability.[31] Availability is a common measure used to identify the amount of time that a service is able to perform its required function, expressed as a percentage. In this case, 99.999% equates to no more than 25.9 seconds of downtime every month. This level of performance is difficult to achieve: Gmail, Google's email product, achieved a 99.978% availability in 2013.[32] Given the level of performance that "Five 9s" describes, it is unlikely that 24th Air Force was suggesting that the

entire Air Force Information Network and its associated services were available everywhere at that availability rate. However, without caveats, it appears to highlight an institutional disconnect: a notably high performance level on a capability for which the Air Force chose corporately to take risk. This may also generate confusion among customers, such as those associated with the CSCS weapon system, who may not perceive their particular experience as reflected in such a high representation of performance. Additionally, this may provide confusing feedback to the Air Force corporate structure on performance possible under an AF COLS 3 level as it suggests the capability can absorb additional resource reductions and still achieve the prescribed output level.

What a Mission Owner Wants

Regardless of any confusion that may exist, it is crucial to understand what mission owners require. Many of them are not cyber professionals, but rely heavily on the capabilities that cyber provides. While they want to understand and manage any risks to their mission, they rely on others to ensure that needed capabilities are available at the required time and place. As the Deputy Commander of U.S. Cyber Command described, "I had a communications staff, and I just told them to make sure my network was always working. Even if there were issues with cybersecurity standards or if we needed to get a waiver, my answer was, 'Yes, just get it in place, just make it work."[33] Regardless of organizational, technical, or other complexities, a mission owner wants their cyber enabling capabilities to work and to have confidence that they will do so. It is understandable that this is the desire of any user of any capability--that it just works.

In the context of the Federal Government, an effort to define "make it work" can start with law. The Federal Information Security Management Act (FISMA) defines the *security*

objectives for information and information systems as confidentiality, integrity, and availability. Confidentiality refers to protecting against "unauthorized disclosure of information."[34] Integrity refers to protecting against the "unauthorized modification or destruction of information."[35] Availability refers to protecting against the "disruption of access to or use of information or an information system."[36] While having the maximum assurance of all three would be the obvious ideal, it is not always possible or practical; however, mission owners can assess the importance of each objective based on expected impact and effectively prioritize. Information systems built to support the mission can consider the relative importance of each security objectives and tailor their design to prioritize those controls that will have the greatest positive impact in ensuring that the system "just works."

Nature of Risk Management

Given the Air Force's reliance on the cyber capabilities and the construct under which we provision and employ those capabilities, it is helpful to have a model for understanding how those capabilities can generate and mitigate risk for the organization and its mission. The following function demonstrates the relationship of the components of risk and how effective risk management results from manipulating them.

Risk = function (threat x vulnerability x impact)

As this formula implies, risk to an organization requires a capable threat that exploits a vulnerability which has an impact. This concept is best expressed as a function to highlight that every mission risk is the result of these three arguments, with each having a direct effect on the resulting risk. For example, if the potential impact is mission failure, then the risk would calculate to a correspondingly high value. Likewise, if a situation exists where there is zero

threat to exploit a specific vulnerability, then that situation represents zero risk to the organization. This model is further effective in developing strategies to address identified threats, since it allows a mission owner to assess whether the threat constitutes any real risk to the organization. Where it does, it helps facilitate development of alternatives to reduce the risk: by reducing the threat, mitigating the vulnerabilities, decreasing the impact, or a combination of all three.

Threat

Threats are anything that contributes to the "tampering, destruction, or interruption of any service or item of value."[37] In other words, threats can range from adversary action to acts of nature and even the well-intentioned actions of an inadequately trained system administrator, so the assessment of threats must consider its motivation in addition to its ability to impose risk. For example, an adversary may be well motivated to access classified logistics systems, but they lack the capability to find and exploit the necessary vulnerabilities. Likewise, a user may have authorized access to a system, but lack motivation to do anything nefarious with it. Other threats are not subject to influence or motivation, such as acts of nature. Some threats exist only as generic characterizations, such as hackers or terrorists, and are not subject to influence until specific actors identify themselves. This will encourage mission owners to focus on the other two arguments of the risk function, over which they have greater control.

Vulnerability

Vulnerabilities are not just those associated with software patches, but can include improper earthquake protection for a datacenter, single points of failure in an architecture, lack

of backup power, or lack of encrypted storage on mobile devices. While it is tempting to focus on information systems, it is crucial to focus on the access and use of information that is necessary to conduct the organization's mission. Additionally, vulnerabilities can exist and be exploited even before they are known to the mission or system owner. Drawing this back to the risk function described above, the value of the vulnerability relates to how costly it is for a threat to exploit it (e.g., a vulnerability that is costly to exploit results in a lower score). Some costs are financial, while others may be expressions of level of effort (e.g., specialized expertise or long development timelines). For example, most software manufacturers regularly release patches to known vulnerabilities. While this process eliminates many known vulnerabilities, it also advertises their existence and provides technical details that make exploiting that vulnerability easier against an unpatched system—resulting in an increased contribution to risk. The longer vulnerabilities are known, the easier and less costly they are to exploit since potential threat actors can leverage the work of others. On the other end of the spectrum, undisclosed vulnerabilities are the costliest since they may require in-house or contracted development work. These undisclosed vulnerabilities are called "zero-days," since the developer has had zero days to create a fix or workaround.[38]

Upon the first exploitation of a vulnerability, a *window of vulnerability* exists until a fix can be developed and applied.[39] During that window, system developers and administrators are racing against potential threats that might exploit the vulnerability to attack a system. This race generates economic forces, which friendly and adversary organizations can exploit. As the DoD Chief Information Officer stated, "from a standpoint of cybersecurity, right now we're on the wrong side of the financial spectrum here…you can spend a little bit of money and a little bit of time and exploit some our [sic] weaknesses, and cause us to have to spend a lot of money, a lot

of time."[40] As an example, zero-day broker Zerodium will pay as much as $1.5 million for "original and previously unreported zero-day exploits."[41] In turn, they sell access to their library of exploits for an annual fee of $500,000 or more.[42] In some cases, these types of sales are large enough to make the news such as when the Director of the Federal Bureau of Investigation indicated that his agency paid more than $1.3 million to access the encrypted iPhone used by an attacker in a mass shooting.[43] Many software companies have their own programs to incentivize people to develop and submit vulnerabilities, with varying rewards available (e.g., Microsoft offers up to $200,000, Google will pay up to $20,000, and Apple up to $200,000).[44] With such legitimate entities willing to pay significant amounts of money for exploits (along with presumably illegitimate ones), there is no shortage of motivation on the supply side of exploit development. This suggests that the only way to influence the market is through demand.[45] While there are indications that demands from government agencies heavily influence the market, most organizations do not have sufficient resources to influence such an expensive market.[46] However, this does not mean they cannot take advantage of it: driving the cost to potential threats as high as possible by denying the use of known vulnerabilities. For commercial products, this means implementing fixes to vulnerabilities as early in the window of vulnerability as possible. For government developed software, program offices must pursue and be accountable to the same goal.

A goal of patching systems as quickly as possible seems intuitive, but vulnerability management continues to be an elusive problem. Predictions are that through the year 2020, 99% of exploits will be based on vulnerabilities that were known for a minimum of one year.[47] According to a Verizon study in 2015, 85% of all exploit traffic was generated by the top 10 vulnerabilities; additionally, more exploited vulnerabilities came from 2007 than any other

year.[48] Even for newer patches, the timelines support the need for deliberate and even aggressive vulnerability management: of the most critical category of Microsoft vulnerabilities identified in 2015, only 5% were believed to have been exploited within 30 days of a patch being available.[49] In 2014, it took software companies an average of 59 days to develop and release patches to vulnerabilities once they were identified.[50] In short, the longer a vulnerability remains, the less costly it is for a threat to exploit; however, once a patch has been developed and published, the cost to mitigate the vulnerability drops precipitously. While zero day vulnerabilities are difficult to counter, there is still substantial benefit in an effective and efficient vulnerability management process—one that decreases risk by increasing the cost to potential threats.

Impact

The impact of a risk to an organization can range from nuisance to mission failure. Businesses reduce impacts to a dollar value that incorporates lost productivity, lost revenue, damage to equipment, unscheduled overtime, etc. For example, data breaches for companies in the United States cost an average of $221 per record ($76 in direct costs and $145 in indirect costs), with each breach averaging a total of $7 million.[51] Armed with this information, companies can make a cost-benefit assessment on any investment that would reduce the risk of a data breach. However, the Air Force does not generate revenue and is not in competition for business, so it cannot necessarily use impacts to the bottom line as an effective means of assessing impact. For example, it is difficult to quantify the impact of a network outage that interrupts dissemination of missions to geographically dispersed units. It is also difficult to compare that to an Air Force-level issue preventing access to email across the entire service. Both issues would cause significant impact, but it would be difficult to objectively determine

which issue is more significant in order to prioritize responses and investment to reduce the risk of recurrence.

Evaluation of mission risk must be from the perspective of the various mission owners that exist in the Air Force. For example, from the perspective of a contracting unit, the network is a vulnerability for their mission effectiveness. If the network, or one of its services (e.g., email), is unavailable, that may have a significant impact on their mission. While this scenario may not be significant in the context of the entire Air Force, it may be significant at a local level. In an organization as large as the Air Force, lost productivity for a minor issue can be significant when extrapolated out to the entire population. For example, it would arguably be worth $17 million to address an issue that costs one hour of time from every uniformed member of the Air Force, since that is the appropriated cost of one hour of the Air Force's payroll.[52] Air Force leadership has said that they "don't care how you get your email…that's not a fundamental mission of the Air Force."[53] Mission owners might agree that reliability from wherever email comes from is more important.

Managing Cyber Risk

Effective risk management requires a mission owner to assess the risks throughout their operation and address those where the impact of a risk is greater than the cost to mitigate the risk.[54] This is analogous to the physical world where the Air Force applies antiterrorism measures, force protection concepts, and Protection Levels to critical resources since the cost of implementing such measures is less than the cost of losing the resource. Organizations will naturally seek to address as many risks as they can afford, based on an understanding of what

missions are important to them and what functions support those missions. In the case of cyber, the most important capabilities are those that support a mission owner's critical functions.

Since many mission owners leverage the same cyber capabilities, the service provider must understand all the dependences on their service. For AF-wide capabilities provided by a single provider, it would be a complex endeavor to maintain a characterization of each dependency such that they can prioritize service. This would require a level of understanding of dependence that exceeds the Air Force's current ability to provide visibility into those same capabilities. In terms of the AFNet, there are certain key elements of the architecture that are dependencies for a large segment of the Air Force—things like connection off the installation, enterprise services, and access to functional applications. This would mean that these core capabilities would need to perform sufficiently to satisfy all the dependent missions.

MORE THAN AN ACADEMIC ARGUMENT

CCRI Results

One place that the confusion on cyber is apparent in the Air Force is in external inspections of its networks. On a recurring pattern of approximately every two years, the Defense Information Systems Agency (DISA) completes assessments of every network in the DoD. This assessment, called a Command Cyber Readiness Inspection (CCRI), is under the authority of United States Cyber Command to evaluate and improve the security of the DODIN.[55] A CCRI evaluates processes, culture, physical security, and the current security state of the network—among other things, ensuring that all networked devices are properly patched, configured, and protected. Unfortunately, the amount of work necessary to achieve a passing score is unsustainable.[56] Units divert resources away from day-to-day operations to prepare for the

inspection, only to have the higher (i.e., required) state of security decline immediately after the inspection.[57] The expressed intent is to move away from an inspection-focused readiness model, to a day-to-day approach where repeatable processes, training, policies, and technology are leveraged to ensure the Air Force is always secure and effectively inspection-ready at any time.[58] A summit was organized by the 690th Cyber Operations Group to identify the root causes of the Air Force's inability to maintain the desired posture: 20 items were identified (two training and six each for processes, technology, and policy).[59] Counter to the results of this work, seven months later the problem was categorized by the 24th Air Force commander as "training, experienced manpower and leadership" with a statement that "the tools work fine … and [are] quite effective."[60] Despite the number of issues identified by the subject matter experts, there appears to be a significant disconnect between those that perceived a problem and those that can make it a priority. Until resolved, that disconnect will likely prevent significant improvement—meaning that cybersecurity is a priority throughout the organization, but the result is cyber insecurity by DoD standards.

Institutional Frustration

In addition to immature/unsustainable security processes, organizations and individuals within the Air Force have indicated that the availability and reliability of enterprise services are not sufficient. As one senior leader described it when speaking at Air War College, "the worst thing I can do for my productivity is turn on my computer in the morning."[61] Several other senior leaders categorized it similarly.[62] In general, such leaders have executive communications support, which provides them with more responsive service than the normal user—making it

logical to assume that their described experience is better than the average. Concerns also extend beyond the individual complaints.

Currently there are entire Air Force organizations that are looking for options outside the AFNet. For example, Air University is moving to Air University Commercial Internet Services (AUCIS). AUCIS "reduces a current gap in learning productivity…by providing increased accessibility to … educational content with high bandwidth requirements on decidedly restrictive government managed networks."[63] Additionally, the 618th Air Operations Center is pursuing options to alter its architecture to decrease its dependence on AFNet resources. Air Force Special Operations Command has also announced their intent to move away from the AFNet, as it cannot meet their mission requirements.[64] Taken together, these three organizations represent a full range of mission criticality with regards to cyber capabilities. If the AFNet is not capable of meeting operational or educational needs, nor meet the expectations of individual Airmen, it is logical to ask, "what organizations is the AFNet intended to support?"

RECOMMENDATIONS

Consolidation of AFNet Sustainment

If everyone is responsible, then no one is responsible. This adage is just as applicable to cyber as it is to organizational management. The Air Force should continue to consolidate responsibility for the acquisition and sustainment of information technology. Presumably this responsibility will continue to align with AFLCMC, given their extensive role in the management of multiple information technology-based capabilities.

Regardless of where consolidated responsibility resides, performance accountability and visibility must increase. While AFLCMC can formally be accountable to a lead command, such

as AFSPC or AFIMSC, they must also make their program performance assessments available to a wider audience. Program managers should invite every MAJCOM/A6 to participate in formal program reviews to ensure the programs continue to meet mission requirements and enable them to advocate for resources as needed. A component of this visibility must also include published service levels for enterprise capabilities to inform the risk considerations of the mission owners throughout the Air Force. A published expectation can facilitate an informed discussion of how to resolve disconnects with mission requirements, providing additional options to address the shortfall.

The Air Force's Chief of Information Dominance and Chief Information Officer has announced that the Air Force is moving to an "As a Service" environment.[65] The consolidation efforts discussed above do not preclude that concept, nor does it preclude outsourcing those services. In fact, continued consolidation helps expose the true cost of information technology requirements in the Air Force and enables a better-informed cost-benefit analysis of such options.

Model for Enterprise Visibility

In addition to improved visibility into the programmatic aspects of providing cyber capabilities, visibility of operational status to mission owners must improve. Visibility of all operational aspects at and from all levels will increase understanding throughout the enterprise and increase accountability, since organizations can address concerns over performance based on the same information and they can make data-driven decisions to address any shortfalls.

As discussed previously, this visibility must incorporate those capabilities that contribute to confidentiality, integrity, and availability. This enables mission owners to better understand

their current risk profile and allows them to make risk-based decisions to mitigate any concerns to their operations. Confidentiality, integrity, and availability are also the criteria used assess systems in the Risk Management Framework, the process used to authorize information systems to operate. The process assists programs in selecting controls to support the required security level of the system and assesses their effectiveness in doing so.[66] The Air Force could extend the use of this model to operational units and facilities, providing a general characterization of the requirements of mission owners—providing data from which cyber operations and sustainment efforts can derive the risk caused by developments in cyberspace and providing a means to communicate the impact to mission owners. Such transparency on requirements and performance will facilitate improved interaction between mission owners and the various entities that have responsibilities in providing cyber capabilities.

In addition to visibility, assessment of impact must also improve. While the above provides a means to communicate changing conditions within cyberspace, the Air Force must establish a common frame of reference to assess the impact of changes on Air Force networks, both positive and negative. One measure to assess impact would be to sum the costs associated with productivity and any loss or required investment. For example, organizations could measure the costs of an unscheduled outage in terms of lost productivity (normalized to a dollar value) and any other costs incurred to continue operations despite the outage. Such a construct could help objectively assess the impact of issues, ensuring that capability providers prioritize issues with the greatest magnitude of impact—including considerations of cost to mission, loss of productivity, etc. Such a measure could also serve to objectively determine if incidents warrant a formal investigation to determine root cause. Additionally, program managers could use the

measure to assess potential improvements to the network and to help justify the cost of their implementation.

Federation of Authority

The Air Force should conduct a comprehensive review to determine if organizations conducting cyber operations, to include installation-level communications squadrons, have the authority, responsibility, and accountability to conduct their required tasks. While considering the concept of least privilege, the Air Force must leverage and facilitate the cyber professionals at all levels and enable them to conduct actions that currently only a select few can take. While concerns over risk often drive a restrictive posture, decision makers must also consider the benefits gained in the increased number of people able to complete a task and flexibility to adapt to local priorities—allowing local commanders to balance mission and technical risks.

Installation-Level Capabilities

Continue to pursue opportunities to provide more capability and flexibility to commanders and mission owners through efforts like the Cyber Squadron Initiative and deployment of the Mission Defense Team – Tool Kit to provide additional capabilities at the unit level. However, decision makers must ensure that they communicate to mission owners that the new capabilities are additive and evolutionary, not a substitute for the performance of legacy information technology services.

CONCLUSION

Much of the cyber capabilities that enable mission owners to function are outside their influence and often outside their visibility. This situation exists because of the confusing nature of "cyber," how the Air Force has evolved cyber capabilities, significant institutional disconnects, what a mission owner wants, and the nature of risk management. The consequences of these issues are more than academic concerns as they have contributed to tangible issues throughout the Air Force. At present, it appears that there is a disconnect between the state of cyber capabilities from the perspective of the user and that of key leaders in positions to exert great influence on the future of cyber in the Air Force. While the Air Force likely cannot afford to meet every organization's desired level of performance, it can ensure that it closes the gap between actual performance and the assessed level of performance—ensuring that programmatic and operational decisions are based on a shared understanding of reality. Such transparency and shared understanding will also provide additional accountability at all levels of cyber operations. This will facilitate informed discussions that can ensure authorities and responsibilities remain aligned with mission requirements, but still balanced with accountability for performance.

Notes

[1] United States Air Force, *Air Force Information Dominance Flight Plan: The Way Forward for Cyberspace/IT in the United States Air Force*, May 1, 2015, 5.
[2] Derived from the research topic submitted by ACC/A6 titled "AF-Wide Cyber Mission Awareness." Question was found in Air University Research Topics 201608220800, sequence number 57, index 126.
[3] Ibid.
[4] Citation needed
[5] JP 3-12 (R). 2013. *Cyberspace Operations*, February 5, GL-4. Also incorporated into JP 1-02. n.d. *DOD Dictionary of Military and Associated Terms.* http://www.dtic.mil/doctrine/dod_dictionary/.
[6] JP 3-13. 2014. *Information Operations*, November 20, GL-3. Also incorporated into JP 1-02.
[7] JP 3-12 (R), vii.
[8] JP 3-12 (R), GL-4. As quoted, the definition was changed from "… information networks" to "… information network." The plural form originated in JP 3-12, but was superseded by JP 6-0 and has not been updated in JP 1-02. The change was made to reduce confusion and maintain consistency with JP 6-0 correction of the plural/singular nature of the term.
[9] JP 6-0, *Joint Communications System*, June 10, 2015, GL-5. Department of Defense information network (DODIN) is defined as The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems."
[10] Department of Defense, *The DoD Cyber Strategy*, April 17, 2015, Foreword.
[11] Ibid.
[12] United States Air Force, *Air Force Information Dominance Flight Plan*. The document repeatedly uses both "IT/Cyberspace" and "Cyberspace/IT."
[13] DoD Instruction 8500.01, *Cybersecurity*, March 14, 2014, 1.
[14] United States Air Force, *Air Force Officer Classification Directory,* October 31, 2016, 78-79.
[15] Pellerin, Cheryl. "CIO Priorities Include Cybersecurity, Innovation, Retaining IT Workforce." *DoD News.* March 23, 2016. Accessed December 4, 2016. https://www.defense.gov/News/Article/Article/702488/cio-priorities-include-cybersecurity-innovation-retaining-it-workforce.
[16] Halvorsen, Terry. *Statement by Terry Halvorsen, Acting Department of Defense Chief Information Officer.* Testimony, Washington, D.C.: House Armed Services Committee, 2015, 1.
[17] Air Force Installation and Mission Support Center [AFIMSC], Operations Support Division. "AFIMSC Communications Capability Update." December, 2016. Extracted from FOUO briefing; permission to and release this slide was obtained from AFIMSC/PA via AFIMSC/IZSS.
[18] United States Air Force, "Air Force Installation and Mission Support Center," *Air Force Installation and Mission Support Center Fact Sheet.* January 8, 2015, Accessed April 3, 2017, http://www.afimsc.af.mil/AboutUs/FactSheets/Display/tabid/5221/Article/559864/af-installation-mission-support-center.aspx.
[19] Ibid.

[20] Olson, Craig. 2014. "New Horizons 2014, C3I & Networks PEO." *AFCEA Boston.* February 25. Accessed April 02, 2017. http://www.afceaboston.com/documents/documents-briefings/hn_nh_2014_final.pdf, 21.
[21] Tinker Air Force Base, "38th Cyberspace Engineering Installation Group Fact Sheet," *Tinker Air Force Base,* February 20, 2014, Accessed April 3, 2017. http://www.tinker.af.mil/AboutUs/FactSheets/Display/tabid/6598/Article/845243/38th-cyberspace-engineering-installation-group.aspx.
[22] Skinner, Robert J, "The Importance of Designating Cyberspace Weapon Systems," *Air and Space Power Journal* 27 (5 (September-October 2013)): 29-48, http://www.au.af.mil/au/afri/aspj/digital/pdf/issues/2013/ASPJ-Sep-Oct-2013.pdf, 30. At the time this article was written, the author was Deputy Commander, Air Forces Cyber.
[23] Ibid, 42.
[24] Ibid, 39.
[25] Comment based on the 561 NOS Mission Briefing, which was provided to the author by its commander.
[26] United States Air Force, "Air Force Common Output Level Standards (AF COLS) Overview," *AF COLS,* January 1, 2017. Accessed February 1, 2017, https://cs1.eis.af.mil/sites/AFCOLS/FY17Playbook/default.aspx.
[27] Ibid.
[28] Ibid.
[29] Vice Chief of Staff, "FY16 Air Force Installation Support Standards," November 12, 2015, Attachment 1.
[30] United States Air Force, n.d., "Current FY AF COLS Levels," *AF COLS,* Accessed February 3, 2017, https://cs1.eis.af.mil/sites/AFCOLS/FY17 Playbook/Pages/Current_FY_AFCOLS_Levels.aspx.
Vice Chief of Staff, "FY16 Air Force Installation Support Standards," Attachment 1.
Chief of Staff, "Air Force Installation Support Standards (HQ USAF/CV Memo, 13 Sep 2012)," January 12, 2013, Attachment.
[31] Fact was noted by the author when attending a briefing at 24 AF on 9 Nov 2016.
[32] Lidzborki, Nicolas, "Staying at the forefront of email security and reliability: HTTPS-only and 99.978 percent availability," *Google Official Blog.* March 20,2014, Accessed April 2, 2017, https://googleblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html.
[33] Serbu, Jared, "Penalty for commanders who negelect cyber: disconnection from DoD networks." *Federal News Radio,* September 21, 2015, Accessed January 15, 2017. http://federalnewsradio.com/defense/2015/09/penalty-military-commanders-neglect-cyber-disconnection-dod-networks/.
[34] FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, 2.
[35] Ibid.
[36] Ibid.
[37] Bayne, James, "An Overview of Threat and Risk Assessment," *SANS Institute,* 2002, Accessed January 31, 2017, https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76, 6.
[38] Zetter, Kim, "Hacker Lexicon: What Is a Zero Day?" *WIRED,* November 11, 2014, Accessed January 31, 2017, https://www.wired.com/2014/11/what-is-a-zero-day/.

[39] Wikipedia, "Zero-day (computing)," *Wikipedia,* Accessed January 31, 2017. https://en.wikipedia.org/wiki/Zero-day_(computing).
[40] Pomerleau, Mark, "DOD to invest heavily in cyber, although details are murky," *Defense Systems,* February 3, 2016, Accessed February 2, 2017, https://defensesystems.com/articles/2016/02/03/dod-cyber-spending.aspx.
[41] ZERODIUM, "Our Exploit Acquisition Program," *ZERODIUM,* Accessed January 31, 2017, https://www.zerodium.com/program.html.
[42] Greenberg, Andy, "Here's a Spy Firm's Price List for Secret hacker Techniques," *WIRED,* November 18, 2015, Accessed January 31, 2017, https://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/.
[43] Lichtblau, Eric, and Katie Benner, "F.B.I. Director Suggests Bill for iPhone Hacking Topped $1.3M," *The New York Times,* April 21, 2016, Accessed January 31, 2017, https://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html.
[44] Microsoft Security Response Center, "Microsoft Bounty Programs," *Microsoft,* Accessed January 31, 2017, https://technet.microsoft.com/en-us/library/dn425036.aspx.
Google, "Google Vulnerability Reward Program (VRP) Rules," *Google,* Accessed January 31, 2017, https://www.google.com/about/appsecurity/reward-program/.
[45] Mueller, Milton, "Regulating the Market for Zero-Day Exploits: Look to the Demand Side," *Internet Governance Project,* March 15, 2013, Accessed December 4, 2013, http://www.internetgovernance.org/2013/03/15/regulating-the-market-for-zero-day-exploits-look-to-the-demand-side/.
[46] Zetter, Kim, "Hacker Lexicon: What Is a Zero Day?" *WIRED,* November 11, 2014, Accessed January 31, 2017, https://www.wired.com/2014/11/what-is-a-zero-day/.
[47] Panetta, Kasey, "Gartner's Top 10 Security Predictions 2016," *Gartner,* June 15, 2016, Accessed January 31, 2017, http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/.
[48] Verizon, *2016 Data Breach Investigations Report,* Report, Verizon, 2016, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.
[49] Microsoft, *Microsoft Security Intelligence Report, Vol 21 (January through June 2016),* Microsoft, 2016, https://www.microsoft.com/security/sir/default.aspx.
[50] Park, Roger, "Guide to Zero-Day Exploits," *Symantec,* November 9, 2015, Accessed January 31, 2017, https://www.symantec.com/connect/blogs/guide-zero-day-exploits. This blog entry is a summary of the Symantec 2015 Internet Security Threat Report, Vol 20).
[51] Ponemon Institute, *2016 Cost of Data Breach Study: United States,* Research Report, IBM, 2016, 2.
[52] Under Secretary of Defense (Comptroller), "FY 2017 Department of Defense (DoD) Military Personnel Composite Standard Pay and Reimbursement Rates," March 9, 2016, http://comptroller.defense.gov/Portals/45/documents/rates/fy2017/2017_k.pdf.
United States Air Force, "FY16 Air Force Strength (Air Force Strength from FY 1948-2016)," *Air Force Personnel Center,* Accessed February 1, 2017, http://access.afpc.af.mil/vbinDMZ/broker.exe?_program=DEMOGPUB.static_reports.sas&_service=pZ1pub1.
Figure was calculated based on the hourly rate from the Comptroller memo and the current strength reference.

[53] Roeder, Tom, "General: 'A hard path' to modernizing military computing," *Colorado Springs Gazette*, February 5, 2015, Accessed January 8, 2017, http://gazette.com/general-a-hard-path-to-modernizing-military-computing/article/1545771.
[54] White, Gregory B., Eric A. Fisch, and Udo W. Pooch, *Computer Systems and Network Security,* Boca Raton: CRC Press, Inc: 1996, 10.
[55] Tyndall Air Force Base, "Command Cyber Readiness Inspection," *Tyndall Air Force Base,* Accessed January 31, 2017, http://www.tyndall.af.mil/AboutUs/CommandCyberReadinessInspection.aspx.
[56] Cyber Ready 365 Summit, "Cyber Ready 365 Game Plan," May 2016, 3.
[57] United States Air Force, "Cyber Ready 365 Working Group Charter." September 1, 2016, 2.
[58] Ibid
[59] Cyber Ready 365 Summit, "Cyber Ready 365 Game Plan," 4
[60] Email sent by 24th Air Force Commander and obtained by the author under condition of non-attribution.
[61] Briefing in Jones Auditorium, 1 Feb 2017. Presentations in Jones Auditorium are conducted under the standard of non-attribution.
[62] Senior Air Force leader presentation in Jones Auditorium. Presentations in Jones Auditorium are conducted under the standard of non-attribution.
[63] Air University, "What is the purpose of AUCIS?" *AU Education Support Center,* December 1, 2016, Accessed February 2, 2017, http://www.aueducationsupport.com/link/portal/8027/8405/Article/6341/What-is-the-purpose-of-AUCIS.
[64] Comments were made by Col Corey Ramsby, AFSPC Chief of Cyberspace Operations, and provided to the author in an email on 1 Mar 2016 by Mr Panayotis Yannakogeorgos, Dean of the Air Force Cyber College.
[65] Bender, William J., "SAF/CIO A6 Mission Brief," *Office of Information Dominance and Chief Information Officer,* Accessed November 29, 2016, http://www.safcioa6.af.mil/Portals/64/documents/SAFCIOA6_Mission%20Brief_Jan2017_Final-feb.pptx?ver=2017-02-10-082415-113, slide 8.
[66] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April, 2013, Chapter 2, page 9.

Bibliography

561 NOS. n.d. "561 NOS Mission Briefing."

AFGM 2016-17-01. 2016. *Communications Squadron-Next (CS-N) Pathfinders,* August 12.

Air Force Installation and Mission Support Center [AFIMSC], Operations Support Division. 2016. "AFIMSC Communications Capability Update." December.

Air University. 2016. "What is the purpose of AUCIS?" *AU Education Support Center.* December 1. Accessed February 2, 2017. http://www.aueducationsupport.com/link/portal/8027/8405/Article/6341/What-is-the-purpose-of-AUCIS.

Bayne, James. 2002. "An Overview of Threat and Risk Assessment." *SANS Institute.* Accessed January 31, 2017. https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76.

Bender, William J. n.d. "SAF/CIO A6 Mission Brief." *Office of Information Dominance and Chief Information Officer.* Accessed November 29, 2016. http://www.safcioa6.af.mil/Portals/64/documents/SAFCIOA6_Mission%20Brief_Jan2017_Final-feb.pptx?ver=2017-02-10-082415-113.

Case. 2016. *Point Paper on Communications Squadron Next Status,* August 9.

Chief of Staff. 2013. "Air Force Installation Support Standards (HQ USAF/CV Memo, 13 Sep 2012)." January 12.

Courville, Shane P. 2007. *Air Force and the Cyberspace Mission Defending the Air Force's Computer Network in the Future.* Maxwell Air Force Base: Air University.

Cyber Ready 365 Summit. 2016. "Cyber Ready 365 Game Plan." May.

Del Monte, Michael. n.d. "The Economics of Network Security." *JDA Professional Services.* Accessed December 4, 2016. http://www.jdapsi.com/Client/Articles/NetSecurity%20MDEL%20101315.pdf.

Department of Defense Chief Information Officer. 2016. *Department of Defense Information Technology Environment*, August.

Department of Defense. 2016. *DoD Cybersecurity Discipline Implementation Plan*, February.

—. 2012. *Mission Assurance Strategy*, May 7.

—. 2015. *The DoD Cyber Strategy*, April 17.

DoD Directive 3020.40. 2016. *Mission Assurance*, November 29.

DoD Instruction 8500.01. 2014. *Cybersecurity*, March 14.

Evans, Mickey R. 2010. *An Informational Analysis and Communications Squadron Survey of Cyberspace Mission Assurance.* Graduate Research Project, Wright-Patterson Air Force Base: Air Force Institute of Technology.

Fahrenkrug, David T. 2007. "Cyberspace Defined." *The Wright Stuff*, May 17. http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm.

FIPS PUB 199. 2004. *Standards for Security Categorization of Federal Information and Information Systems*, February.

Google. n.d. "Google Vulnerability Reward Program (VRP) Rules." *Google.* Accessed January 31, 2017. https://www.google.com/about/appsecurity/reward-program/.

Greenberg, Andy. 2015. "Here's a Spy Firm's Price List for Secret hacker Techniques." *WIRED.* November 18. Accessed January 31, 2017. https://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/.

Halvorsen, Terry. 2015. *Statement by Terry Halvorsen, Acting Department of Defense Chief Information Officer.* Testimony, Washington, D.C.: House Armed Services Committee.

Jabbour, Kamal, and Sarah Muccio. 2011. "The Science of Mission Assurance." *Journal of Strategic Security* 4 (No. 2). doi:http://dx.doi.org/10.5038/1944-0472.4.2.4.

JP 1-02. n.d. *DOD Dictionary of Military and Associated Terms.* http://www.dtic.mil/doctrine/dod_dictionary/.

JP 3-12 (R). 2013. *Cyberspace Operations*, February 5.

JP 3-13. 2014. *Information Operations*, November 20.

JP 6-0. 2015. *Joint Communications System*, June 10.

JROCM 107-14. 2014. *Capability Production Document for Cyberspace Security and Control System*, October 10.

Kastenberg, Joshua E. 2009. "Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DoD to Take Time-Sensitive Action on the NIPRNET." *The Air Force Law Review* 64 (Cyberlaw Edition).

Kenyon, Henry. 2011. "Air Force embraces new mindset for cyber warfare." *Defense Systems.* February 1. Accessed January 8, 2017. https://defensesystems.com/articles/2011/01/31/air-force-cyber-command-ready-for-operations.aspx.

Lee, Robert M. 2015. "Disruptive by Design: Saving the Air Force Cyber Community." *Signal*, February 1. http://www.afcea.org/content/?q=disruptive-design-saving-air-force-cyber-community.

Lelarge, Marc. 2011. "Network Security: an Economc Perspective." *PSL Research University Paris.* Accessed December 4, 2016. http://www.di.ens.fr/~lelarge/Network_Security_web.pdf.

Libicki, Martin C., Lillian Ablon, and Tim Webb. 2015. *The Defender's Dilemma: Charting a Course Toward Cybersecurity.* Research Project, Santa Monica: RAND Corporation.

Lichtblau, Eric, and Katie Benner. 2016. "F.B.I. Director Suggests Bill for iPhone Hacking Topped $1.3M." *The New York Times.* April 21. Accessed January 31, 2017. https://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html.

Lidzborki, Nicolas. 2014. "Staying at the forefront of email security and reliability: HTTPS-only and 99.978 percent availability." *Google Official Blog.* March 20. Accessed April 2, 2017. https://googleblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html.

Microsoft. 2016. *Microsoft Security Intelligence Report, Vol 21 (January through June 2016).* Microsoft. https://www.microsoft.com/security/sir/default.aspx.

Microsoft Security Response Center. n.d. "Microsoft Bounty Programs." *Microsoft.* Accessed January 31, 2017. https://technet.microsoft.com/en-us/library/dn425036.aspx.

Mueller, Milton. 2013. "Regulating the Market for Zero-Day Exploits: Look to the Demand Side." *Internet Governance Project.* March 15. Accessed December 4, 2013. http://www.internetgovernance.org/2013/03/15/regulating-the-market-for-zero-day-exploits-look-to-the-demand-side/.

NIST SP 800-53. 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, April.

Olson, Craig. 2014. "New Horizons 2014, C3I & Networks PEO." *AFCEA Boston.* February 25. Accessed April 02, 2017. http://www.afceaboston.com/documents/documents-briefings/hn_nh_2014_final.pdf.

Panetta, Kasey. 2016. "Gartner's Top 10 Security Predictions 2016." *Gartner.* June 15. Accessed January 31, 2017. http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/.

Park, Roger. 2015. "Guide to Zero-Day Exploits." *Symantec.* November 9. Accessed January 31, 2017. https://www.symantec.com/connect/blogs/guide-zero-day-exploits.

Pellerin, Cheryl. 2016. "CIO Priorities Include Cybersecurity, Innovation, Retaining IT Workforce." *DoD News.* March 23. Accessed December 4, 2016.

https://www.defense.gov/News/Article/Article/702488/cio-priorities-include-cybersecurity-innovation-retaining-it-workforce.

Pomerleau, Mark. 2016. "Air Force's cyber boss: Military needs to innovate at 'cyber speed'." *Defense Systems.* April 25. Accessed January 8, 2017. https://defensesystems.com/articles/2016/04/25/air-forces-cyber-wilson-innovation-speed.aspx.

—. 2016. "DOD to invest heavily in cyber, although details are murky." *Defense Systems.* February 3. Accessed February 2, 2017. https://defensesystems.com/articles/2016/02/03/dod-cyber-spending.aspx.

Ponemon Institute. 2016. *2016 Cost of Data Breach Study: United States.* Research Report, IBM.

Pope, Billy, and Justin Ellsworth. 2017. *Cyber Squadron Initiative.* February. Accessed April 05, 2017. https://www.milsuite.mil/book/docs/DOC-336912.

Pritchett, Michael D. 2012. *Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment.* Graduate Research Project, Wright-Patterson Air Force Base: Air Force Institute of Technology.

Roeder, Tom. 2015. "General: 'A hard path' to modernizing military computing." *Colorado Springs Gazette.* February 5. Accessed January 8, 2017. http://gazette.com/general-a-hard-path-to-modernizing-military-computing/article/1545771.

Schmidt, Lara. 2015. *Perspective on 2015 DoD Cyber Strategy.* Testimony, RAND Corporation. http://www.rand.org/pubs/testimonies/CT439.html.

Schmidt, Lara, Caolionn O'Connell, Hirokazu Miyake, Akhil R. Shah, Joshua William Baron, Geof Nieboer, Rose Jourdan, et al. 2015. *Cyber Practices: What Can the U.S. Air Force Learn from the Commercial Sector?* Research Report, Santa Monica: RAND Corporation.

Serbu, Jared. 2015. "Penalty for commanders who negelect cyber: disconnection from DoD networks." *Federal News Radio.* September 21. Accessed January 15, 2017. http://federalnewsradio.com/defense/2015/09/penalty-military-commanders-neglect-cyber-disconnection-dod-networks/.

Skinner, Robert J. 2013. "The Importance of Designating Cyberspace Weapon Systems." *Air and Space Power Journal* 27 (5 (September-October 2013)): 29-48. http://www.au.af.mil/au/afri/aspj/digital/pdf/issues/2013/ASPJ-Sep-Oct-2013.pdf.

Snyder, Don, George E. Hart, Kristin F. Lynch, and John G. Drew. 2015. *Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems.* Research Report, Santa Monica: RAND Corporation.

Snyder, Don, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, and Michael H. Powell. 2015. *Improving the Cybersecurity of U.S. Air Force Military*

Systems Throughout Their Life Cycles. Research Project, Santa Monica: RAND Corporation.

Snyder, Don, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, and Michael H. Powell. 2015. *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles.* Research Report, Santa Monica: RAND Corporation.

Sweeney, Patrick. n.d. "Network-based attacks: How much can they cost you?" *SC Magazine US.* Accessed December 4, 2016. https://www.scmagazine.com/network-based-attacks-how-much-can-they-cost-you/article/541922/.

Takanen, Matthew. 2016. "Mission Defense Teams: Persistent Cyber Defense for ACC Weapons Systems/Platforms." October 20.

The Economist. 2013. "The digital arms trade." March 30. Accessed December 4, 2016. http://www.economist.com/node/21574478.

The MITRE Corporation. 2014. *Systems Engineering Guide.* Systems Engineering Resource, Bedford: The MITRE Corporation. https://www.mitre.org/publications/technical-papers/the-mitre-systems-engineering-guide.

Tinker Air Force Base. 2014. "38th Cyberspace Engineering Installation Group Fact Sheet." *Tinker Air Force Base.* February 20. Accessed April 3, 2017. http://www.tinker.af.mil/AboutUs/FactSheets/Display/tabid/6598/Article/845243/38th-cyberspace-engineering-installation-group.aspx.

Tyndall Air Force Base. n.d. "Command Cyber Readiness Inspection." *Tyndall Air Force Base.* Accessed January 31, 2017. http://www.tyndall.af.mil/AboutUs/CommandCyberReadinessInspection.aspx.

Under Secretary of Defense (Comptroller). 2016. "FY 2017 Department of Defense (DoD) Military Personnel Composite Standard Pay and Reimbursement Rates." March 9. http://comptroller.defense.gov/Portals/45/documents/rates/fy2017/2017_k.pdf.

United States Air Force. 2016. *Air Force Officer Classification Directory.* October 31.

—. 2017. "Air Force Common Output Level Standards (AF COLS) Overview." *AF COLS.* January 1. Accessed February 1, 2017. https://cs1.eis.af.mil/sites/AFCOLS/FY17Playbook/default.aspx.

—. 2015. *Air Force Future Operating Concept: A View of the Air Force in 2035*, September.

—. 2015. *Air Force Information Dominance Flight Plan: The Way Forward for Cyberspace/IT in the United States Air Force*, May 1.

—. 2015. "Air Force Installation and Mission Support Center." *Air Force Installation and Mission Support Center Fact Sheet.* January 8. Accessed April 3, 2017.

http://www.afimsc.af.mil/AboutUs/FactSheets/Display/tabid/5221/Article/559864/af-installation-mission-support-center.aspx.

—. n.d. "Current FY AF COLS Levels." *AF COLS.* Accessed February 3, 2017. https://cs1.eis.af.mil/sites/AFCOLS/FY17 Playbook/Pages/Current_FY_AFCOLS_Levels.aspx.

—. 2016. "Cyber Ready 365 Working Group Charter." September 1.

—. n.d. "FY16 Air Force Strength (Air Force Strength from FY 1948-2016)." *Air Force Personnel Center.* Accessed February 1, 2017. http://access.afpc.af.mil/vbinDMZ/broker.exe?_program=DEMOGPUB.static_reports.sas&_service=pZ1pub1.

Verizon. 2016. *2016 Data Breach Investigations Report.* Report, Verizon. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

Vice Chief of Staff. 2015. "FY16 Air Force Installation Support Standards." November 12.

Welsh, Patty. 2016. "General highlights importance of constructing C2 for networks." *United States Air Force.* October 3. Accessed January 8, 2017. http://www.af.mil/News/ArticleDisplay/tabid/223/Article/962149/general-highlights-importance-of-constructing-c2-for-networks.aspx.

White, Gregory B., Eric A. Fisch, and Udo W. Pooch. 1996. *Computer Systems and Network Security.* Boca Raton: CRC Press, Inc.

Wikipedia. n.d. "Zero-day (computing)." *Wikipedia.* Accessed January 31, 2017. https://en.wikipedia.org/wiki/Zero-day_(computing).

ZERODIUM. n.d. "Our Exploit Acquisition Program." *ZERODIUM.* Accessed January 31, 2017. https://www.zerodium.com/program.html.

Zetter, Kim. 2014. "Hacker Lexicon: What Is a Zero Day?" *WIRED.* November 11. Accessed January 31, 2017. https://www.wired.com/2014/11/what-is-a-zero-day/.